BISNES.FI

Ref.: 03/bfi0864c Grade: 3

Printed by: typing Pages: 18

Translation: Jaakko Mäntyjärvi, Diana Tullberg /British

http://www.englishcentre.fi/ E-mail: desk@englishcentre.fi

2002-09-14 / 01:00 **VIRUS STRIKE**

It took the F-Secure virus lab four hours to come up with a disinfectant for the Slapper worm. Future super viruses may only allow for a response time of 15 seconds.

Text: Juha-Matti Mäntylä
Illustrations: Kustaa Saksi
Photos: Henna Aaltonen

Friday. "For some reason, worms usually appear on a Friday," says Mikko Hyppönen, Antivirus Research Manager at F-Secure.

It seems to be a rule of thumb for virus authors to release self-replicating server-to-server worms just when most virus specialists and corporate IT staff are heading home for the weekend, while viruses propagated through e-mail are released at the beginning of the week to maximize their effect, clogging up e-mail systems for days on end.

The two most significant virus epidemics of the past year, the Slapper worm and the Bugbear e-mail virus, were textbook cases in this respect. Slapper was released on the night of Saturday, September 14, 2002, while Bugbear appeared on Monday, September 31, 2002, when most virus specialists were on their way home from a major professional seminar in the field in New Orleans.

The tactics of virus specialists rely on anticipation and non-disclosure. Macro viruses had been discussed in limited circles for some years before the first virus author came up with the idea in 1995.

Anticipation is combined with readiness. Of the eight virus researchers employed by F-Secure, three are on call next to a phone and a computer at all times. If something happens during the night, the US office wakes them up.

When an epidemic starts, everything comes down to response time. The clock starts ticking at the moment the company receives a sample of a new virus and stops when an update to disinfect that virus is published. Customer agreements stipulate a maximum response time of 12 hours. Hyppönen's team clocks in at an average of two and a half hours.

Process. "How does an antivirus lab work?" Hyppönen repeats the question. "It's not something we usually talk about. People in the field rarely publicize their processes."

He opens the locked door to the antivirus lab on the fourth floor. No other journalist has been in here before except for a reporter from Focus magazine in Germany.

Hyppönen, 33, joined the company 12 years ago when it was still "very much a student project". Today, the company employs over 300 people, and the three-tier alert classification of the antivirus lab is chillingly reminiscent of the DefCon classification of preparedness for nuclear war in American war films.

Inside, no fog or cobwebs can be seen, nor eerily lit screens. The room is brightly lit and empty.

Long rows of computers are lined up against two walls. One set is for testing antivirus database updates to be sent to customers. The other set can be used to simulate a real corporate network to test its strength.

The computer used to publish database updates for customers is in a sealed cabinet. The update keys are kept in a safe. None of the other computers is connected to the Internet.

Fighting viruses is a game of trust. The strict regulations stipulate that no CD-ROMs or other storage media may be removed from the room.

On the day before the interview, the system of Kaspersky Labs in Moscow was invaded. A cracker humiliated the company by sending a virus alert in the company’s name to its customers. The alert itself contained the virus in question.

Hyppönen admits that this is one of the most terrible things that can happen to a data security company. “Fortunately, they had already released an update which disinfected that particular worm, so the customers’ computers weren’t really at risk.”

The eight virus specialists at F-Secure each have their own speciality, such as Windows binaries, Linux, macros, scripts or mobile terminal devices.

“I’m in charge of the lab, and Katrin Tocheva, a Bulgarian who has been with us for five years, is the team manager. She’s responsible for publishing updates. Alexey Podrezov is a former McAfee employee recruited four years ago. He’s in charge of the Windows side. Gergely Erdélyi is a Linux guru from Hungary who joined two and a half years ago. He was a major player in the Slapper case. Ero Carrera from Spain is a junior virus specialist whose strength is also Linux,” Hyppönen describes his team members.

“We only do research, publish updates and issue alerts. The other 310 people in the company manage everything else.”

The lab’s e-mail boxes show that the specialists receive messages, queries and samples at the rate of a few every hour from all over the world. Every sample must be investigated.

“Most virus samples come from the field, either from our paying customers or people who use the freeware version of our software. Often it’s these enlightened home users who first encounter new viruses, and because of that they’re very important to us,” Hyppönen says. “The rest of the samples come from other virus labs through a sample exchange programme.”

Once a virus sample has been received, it is analysed to find a unique segment of code, typically its replication routine. “This means finding a bit of code that you’d never find in a clean copy of any legitimate software. Then we devise an identification routine, test it and release it to the world,” Hyppönen says.

Each update is delivered to F-Secure’s own customers and to ISPs who use F-Secure to provide data security services for their customers.

Friends and enemies. When the talk turns to night-time operations, 24-year-old virus specialist Gergely Erdélyi glances at his colleague Ero Carrera and quips that they have no life. Both are wearing bright red F-Secure T-shirts.

“Being ready all the time is part of the job. It’s like being a policeman or a doctor.”

Response time is a merciless indicator.

“I began working with viruses six years ago. At that time, it could take months or even a year for a virus to become widespread. Now it’s a matter of days or even of minutes. A crisis is like running through a dark forest without knowing what’s there. A virus may be excruciatingly difficult to analyse, but it has to be done. The reward is a feeling of a job well done,” Erdélyi explains.

It is easy to understand that young men enjoy challenges. But Erdélyi does not say that viruses are the best part of his job.

“You couldn’t really say that,” he grins. “But it’s an adrenaline rush, I have to say. The critical thing is that you have to stand the pressure.”

Hyppönen likes to talk about his lab’s response times. For instance, in the case of the Goner worm, F-Secure beat the response time of its next fastest competitor, Trend Micro, by half an hour. Are response times an important criterion for customers?

“I hope so. On the other hand, rapid response is the default. When we do a good job, no one comes to thank us especially. But if it took us a week to release an update, we’d get nasty feedback that would be reflected in the company’s image,” Hyppönen replies.

Although competition between data security companies is tough, virus specialists seem to cooperate closely.

“Companies are bitter rivals in marketing and sales, but there is solidarity between specialists,” Hyppönen agrees.

“It’s in the users’ interest. In the 1980s, there were certain unhealthy phenomena such as someone publishing a notification on a new version of the Jerusalem virus and then sitting on the sample so that no one else could analyse Jerusalem II because no samples were available.”

Today, sample exchange between data security companies is standard practice. For instance, F-Secure received its sample of the Bugbear worm from Symantec in Australia. Collegial cooperation even extends beyond sample exchange.

“It’s about personal relations. If Jimmy Kuo from McAfee rings and asks for advice on how to decode a sample, then of course we’ll help him. I’ve known him for years, and I know that he’d help us too — as indeed he has,” Hyppönen says. “Sure, he works for a competitor, but so what?”

Virus specialists are into networking for the simple reason that there is very little brain capacity in the field. Hyppönen estimates that there are fewer than 100 top specialists in the world, and antivirus research is not taught anywhere.

“Everyone in the field is more or less self-educated through finding out things for himself.”

So virus specialists are self-made men — just like virus authors? But is the latter group growing more quickly?

“Unfortunately, yes. But we can’t go hiring them. You don’t recruit the enemy; that’s been company policy from the very beginning,” Hyppönen says categorically.

Specialists are reluctant to discuss virus authors in any detail. Gergely Erdélyi says he rarely considers what makes them tick.

Nevertheless, an author leaves his mark on his work. “The code conveys a hint of the author’s personality, or at least of his coding skills. You can tell whether the code is well or poorly written,” Erdélyi says.

When data security experts discuss virus authors, a certain amount of esteem can be detected. That seems curious.

Hyppönen admits to thinking about this.

“It’s about the respect of one technical craftsman for another. For example, the virus author known as Dark Avenger was a highly intelligent and skilled code-writer whose every virus did something new,” Hyppönen says. “He’s been gone for a long time now. I think his last virus appeared in 1993.”

No one ever found out who Dark Avenger was, but another technical wizard, the author of the SMEG family of polymorphic viruses, ended up in prison for his efforts.

An impoverished Bulgarian nerd writing brilliant virus code may command some sort of respect among the antivirus community, but a case like Nimda earns nothing but scorn from Hyppönen, even though the virus was skilfully coded.

“It very quickly projected the impression that we were no longer talking about amateurs. It was written by a dedicated group with a motive and an agenda. Naturally such a group can write good code,” Hyppönen fumes.

Super worm. 2001 was the year of the worm. Nimda infected 2.2 million computers in one day, according to Computer Economics, and EUR 535 million was spent in repairing the damage. The most destructive worm of all was Code Red, which caused damage worth EUR 2.6 billion according to one estimate.

This, however, was only a prelude. The computer world is waiting in trepidation for the appearance of ‘flash’ worms.

The term ‘flash’ refers to the rate at which such worms spread.

“The attack network generated by Slapper was a good idea,” says Hyppönen. “Code Red was programmed to attack the White House website on July 19, and once launched it was beyond the control of its author. The author of Slapper, by contrast, had full control of every infected machine all the time through an anonymous channel.”

The distribution routine, however, was rudimentary.

“The way an infected computer began to look for new victims was extremely stupid. It simply generated a random IP address and then checked whether that address had a computer, and if so whether it had the right sort of server, and if so whether it had the right sort of software with a loophole in it. If all these conditions were met, it could infect the server.”

But in 99.99% of cases there was no computer, no server and/or no loophole, and the worm could do no more than generate a new address.

"There are a lot of addresses on the Internet – some 4.2 billion. At that rate, it would take 130 years to run through them all. Of course, this would be cut down because every now and again the worm would find a suitable computer that would then begin spreading the worm as well. But it's slow in any case."

The super worm of the future will be much more intelligent. For example, instead of generating random addresses, it will carry a payload of, say, 10,000 suitable addresses. The author can generate a list of targets by using Google. As the flash worm infects targets, the list is distributed again and again.

"This dramatically increases the rate at which the worm spreads. Instead of days, we're talking about 15 minutes or 15 seconds," Hyppönen says. "With our current response time of two to three hours, we'd be simply nowhere. By the time we had published an update, the worm would have achieved everything it was designed to do and shut down."

Hyppönen sketches the logic of the super worm on a white board as he speaks. All this is theory – so far. But why is he telling us all this? Would it not be better to keep it quiet?

"I wouldn't be telling you this if an academic researcher at Berkeley hadn't published a paper on the subject six months ago. Which I think sucks big time," Hyppönen complains. "Traditionally, such things are not spoken of, because silence slows down virus development and release.

He’s in academia, and he didn’t know that you just don’t say this sort of thing out loud.”

The title of the paper was entitled ‘How to Own the Internet in Your Spare Time’. Its bleak visions are backed up with theory and mathematical formulas. So the cat is out of the bag, and the gauntlet has been thrown down for all the virus authors in the world.

The fear of the entire Internet going down some day is a realistic one. However, Hyppönen is surprisingly calm when he discusses the super worm scenario.

“Oh, it’ll happen all right — it’s only a matter of time. This theory is now being actively discussed in virus author newsgroups, which are very much like the notorious home chemistry forums,” Hyppönen says and pauses to think.

“But even in the worst case scenario, this would only bring down the Internet. It wouldn’t blow up nuclear power stations or crash planes.”

Post Mortem: The Super Virus was found on 24th of January 2003. Named Slammer, it scanned all the computers in the public internet in roughly 13 minutes, infecting more than 100 thousand database servers and crashing ATM machines, air traffic control system and emergency phone services.

# # #

Sat 2002-09-14 / 09.00

Senior virus specialist Sami Rautiainen at F-Secure reads his e-mail at home. He is one of the three lab employees on call.

Rautiainen’s attention is drawn by a message sent to an e-mail list on the data security of multinational corporations. The message describes the strange behaviour of a Linux server in Romania.

He scans for signs of a potential new worm. By 11.30, he has found indications on both European and American servers.

He notifies team manager Katrin Tocheva, who rings research manager Mikko Hyppönen.

Sat 2002-09-14 / 12.30

Hyppönen answers the phone. He is at home making lunch.

Linux viruses are still rare, and for this reason Hyppönen takes up the case with Tocheva and Rautiainen even though he is not officially on call.

Sat 2002-09-14 / 12.40

They find that the F-Secure Internet servers are offline because the power has been shut down for maintenance work. The specialists use backup systems and use MSN Messenger and Yahoo Webmail to communicate.

The worm seems to infect Apache web servers whose OpenSSL libraries have not been updated. It exploits a loophole for which a patch has been available for over a month.

Specialists at Symantec in Australia dub the virus ‘Slapper’. The hunt is on. Computers with the right sort of Apache server and a non-updated OpenSSL library are set up as bait.

Sat 2002-09-14 / 13.00

Frisk Software, F-Secure’s product development partner in Iceland, catches the first live sample of the worm and sends it to Finland.

The specialists analyse the code, seeking a characteristic bit to use as a search term in virus scanning. A new antivirus database update is created.

The worm is forming an attack network of the infected computers. The Internet Storm Center service carries a rumour that this network has already attacked an unspecified ISP.

Hyppönen notifies the CERT-FI unit of the Finnish Communications Regulatory Authority (FICORA), which contacts Finnish ISPs.

Sat 2002-09-14 / 13.40

The first analysis of the sample is written and published online. Often, even a 15-line bulletin is enough to help fight the infection even if an antivirus database update is not yet available. After all, in the case of Nimda it was enough to alert administrators to block attachment files named README.EXE.

Sat 2002-09-14 / 15.00

The maintenance work is done, power is restored, and the virus specialists return to their principal workstations.

Sat 2002-09-14 / 15.30

'F-Secure Radar Level 2 Alert'. Hyppönen releases a bulletin on raising the level of readiness. This means that a potentially dangerous virus is on the loose but that the situation is not critical.

Customers subscribing to the Radar service are notified by SMS message.

Sat 2002-09-14 / 16.00

Rautiainen drives to the office and begins testing the new update in the lab.

Sat 2002-09-14 / 16.30

Communication assistant Henrietta Malmari and Mikko Hyppönen decide to issue a press release. Usually this is done only if the readiness is raised to Level 1. This exceptional decision is taken so that IT professionals off duty for the weekend can hear of this new potential threat through the media. The press release is phrased in cautiously concerned tones.

Sat 2002-09-14 / 18.30

Tomi Tuominen, who is responsible for data security in F-Secure’s own systems, floats an unusual idea: “If the worm generates an attack network of infected computers, then wouldn’t it be possible to break into it?”

Hyppönen considers Linux expert Gergely Erdélyi to be the best man for the job. The young Hungarian, who lives in Töölö in Helsinki, was planning to spend the weekend with his girlfriend, but his plans are changed with a call from his supervisor.

Erdélyi is excited by the idea of doing something unusual with a worm in a Linux environment. He begins to reverse engineer the network protocol of the worm.

Sat 2002-09-14 / 19.30

In the lab, Sami Rautiainen finishes testing the update and publishes it. Push technology transfers the packages automatically to customers’ systems. A technical description of the worm is published online.

The response phase is completed when the description, identification and database update with disinfection routine are completed. Four hours and ten minutes have elapsed, 90 minutes more than for an average Windows virus. Hyppönen, however, is satisfied. No one has all that much experience in analysing Linux worms. And it is the weekend, after all.

Sat 2002-09-14 / 22.00

The day is done for everyone except Gergely Erdélyi, who has successfully decoded the worm’s network protocol and begins to code a daemon which would enable the worm’s attack network to be penetrated.

Sun 2002-09-15 / 12.00

Hyppönen is shopping at his local grocery store when a tired Erdélyi rings him and says that the daemon is functional.

Erdélyi has managed to penetrate the worm’s attack network during the night, and now F-Secure is the only antivirus company in the world that knows the exact number of infected computers and their addresses.

Initial figures show that Slapper has infected 5,800 computers. Erdélyi and Hyppönen recall that a 20-server attack brought down Amazon in early 2000.

Sun 2002-09-15 / 16.00

The worm is avoiding the bait computer, which is swapped for another. The IT department reluctantly parts with its network game server, a Linux machine.

Hyppönen rings Risto Siilasmaa, managing director of F-Secure, to review the weekend’s events and to discuss the content of a second press release.

The second press release, issued around 23.00, is more sombre in tone than the first. “A rapidly spreading new Linux worm gives the attacker control of infected computers.”

Mon 2002-09-16 / 10.00

Data security Kauto Huopio at the CERT-FI unit at FICORA rings Hyppönen and reviews the order of play in which information on infected computers may be passed forward. What, for instance, would a data security company do if a list of, say, 900 infected German servers were to fall into the wrong hands and get crammed with porn?

CERT-FI begins to contact Finnish IT administrators by phone.

Mon 2002-09-16 / 13.00

The number of infected computers tops 13,000. The virus specialists have realized that they have the means to dispose of the worm quickly: by entering the infected servers through the same loophole as the worm used, they could issue a kill command.

This, however, would be illegal. The company lawyer considers that they would be guilty of unauthorized server access at the very least.

Instead of implementing this quick fix, the specialists begin contacting the thousands of server administrators involved.

In the course of the day, the four leading antivirus companies — Symantec, Trend Micro, McAfee and Computer Associates — each release a database update.

Mon 2002-09-16 / 16.00

‘F-Secure Radar Upgraded to Level 1’. All scheduled in-house meetings are cancelled. All remaining virus specialists are called in. The entire staff is informed. Administrators in customer companies subscribing to the Radar service are notified by SMS message.

Temps are hired to man the switchboard, and the tapes containing music played for callers on hold are replaced with instructions on how to disinfect the worm. Sales staff contact major customers and tell them what is going on.

Mon 2002-09-16 / 18.00

The number of infected computers has increased by 5,000 to 18,000 in five hours.

A free version of a virus scanner for Linux is published online.

Ero Carrera, acting on instructions from Kauto Huopio, sends the CERT authorities in 13 countries a list of the infected servers.

At 21.00, a mass e-mail is sent to the administrators of 7,000 servers, with instructions on how to disinfect the worm. 2,000 of them are not reached.

Tue 2002-09-17 / 09.00

Users are cleaning up their computers, and the spreading of the worm is halted. The number of infections remains below the 20,000 mark.

A graphic updated every hour is published in the evening, showing the number of servers still infected. There are about 2,000 of them, roughly equal to the number of administrators who were not reached.

Wed 2002-09-18 / 04.00

In the night, a private individual publishes a tool online for killing the worm within the servers. This has been discussed in antivirus news groups for a few days. This is exactly what the company lawyer warned the lab against on Monday.

The impact is dramatic. The number of infected servers drops from 1,400 to about 400 within an hour.

Wed 2002-09-18 /09.00

The number of computers still active in the attack network drops below 200 and eventually to a few dozen. Experts begin debating how serious a threat Slapper actually was.

The weak point of the worm is — surprisingly — data security. For example, communication between infected servers is not encrypted, and information on computers linked to the attack network can easily be retrieved.

Despite its ‘shortcomings’, the peer-to-peer networking capabilities of the worm represent a major step in virus evolution.

Later, Mikko Hyppönen mentions the need to set up an official international organization that would have the authority to perform defensive network actions. The suggestion is met with mixed emotions.

The worm, however, is not yet dead. Its author can still launch denial-of-service attacks with the two dozen or so servers he still controls, which is plenty.

New B and C versions of Slapper appear in subsequent weeks.